Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 121 (2017) 568–575

Procedia Computer Science

www.elsevier.com/locate/procedia

CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies, CENTERIS / ProjMAN / HCist 2017, 8-10 November 2017, Barcelona, Spain

A Comparison of Cybersecurity Risk Analysis Tools

Gabriela Roldán-Molina[a,b*], Mario Almache-Cueva[a], Carlos Silva-Rabadão[b], Iryna Yevseyeva[c], Vitor Basto-Fernandes[b,d]

[a] *Departamento de Ciencias de la Computación, Universidad de las Fuerzas Armadas ESPE, Sangolquí, Ecuador*
[b] *School of Technology and Management,Computer Science and Communications Research Centre, Polytechnic Institute of Leiria, 2411-901 Leiria, Portugal*
[c] *Cyber Technology Institute, School of Computer Science and Informatics, Faculty of Technology, De Montfort University, LE1 9BH Leicester, United Kingdoms*
[d] *Instituto Universitário de Lisboa (ISCTE-IUL), University Institute of Lisbon, ISTAR-IUL, Av. das Forças Armadas, 1649-026 Lisboa, Portugal*

Abstract

This paper presents ongoing work of a decision aiding software intended to support cyber risk and cyber threats analysis of an information and communication technology infrastructure. The work is focused on the evaluation of the most popular and relevant tools available for risk assessment and decision making in the cybersecurity domain. Their properties, metrics and strategies are analysed and their support for cybersecurity risk analysis, decision-making and prevention is assessed for the protection of an organization's information assets.

Peer-review under responsibility of the scientific committee of the CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies.

Keywords: Decision aiding; cibersecurity; risk analysis.

* * Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000 .
E-mail address: gaby_r0805@hotmail.com

1877-0509
Peer-review under responsibility of the scientific committee of the CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies.
10.1016/j.procs.2017.11.075

1. Introduction

In a densely-connected world highly dependent on information and communication, timely and relevant data can provide more informative decision making in any domain, and in cyber security in particular. There are currently software tools able to collect detailed data about the information and communication technology (ICT) infrastructure, and relate this information with cybersecurity data (vulnerabilities, severity, remediation measures, etc.) made available by international cybersecurity authorities. These tools make use of cybersecurity metrics, standards, protocols and strategies to identify, understand and anticipate potential company's cybersecurity problems, and provide valuable guidance for today's corporations information and security management. This article analyses different tools for ICT infrastructure data collection, vulnerability scanning and the support they can provide for cybersecurity risk assessment and decision making in organizations. The criteria used to evaluate, compare and select the most suitable for this study these tools include cybersecurity metrics, standards and risk strategies. In addition, they are classified and contextualized with respect to the situation awareness layer they belong to (perception, comprehension, projection and decision/action). The paper is organized as follows, section 2 presents the tools and section 3 presents a comparative analysis of these tools with respect to risk assessment. Section 4 presents a case study carried out at the Universidad de las Fuerzas Armadas ESPE – Ecuador using Nexpose[15] and section 5 proposes the development of a tool addressing different situation awareness layers, to improve cybersecurity organizational decision-making ability. Finally, section 6 presents the conclusions and future work.

2. ICT infrastructure and cybersecurity data collection tools

Following a detailed literature review on most relevant ICT infrastructure and cybersecurity data collection tools, and having proceeded with an initial shortlisting process, we reached a set of nine tools of interest to be addressed in our study: Nessus, Saint8, Retina Security Scanner, GFI LANGuard, nCircle® IP360, Security System Analyzer 2.0, OpenVas, QualysGuard, Nexpose. These tools were analyzed according to the following criteria, which are assumed in our study as the most relevant for the tools comparison: cybersecurity metrics (confidentiality, integrity impact, etc.), standards (CVE, CVSS, etc.) and risk strategies supported (real, temporal, weighted). These tools are presented next.

Nessus[1] supports the Common Vulnerability Scoring System (CVSS) standard[19], including metrics from versions v2 and v3 simultaneously. If both CVSS2 and CVSS3 attributes are present, both scores are computed. However, when computing risk factor, the CVSS2 score takes precedence. Besides, Nessus includes a risk factor based on CVSS which filters results based on the vulnerabilities detected in the ICT infrastructure (e.g., Low, Medium, High, Critical). The severity ratings are derived from the associated CVSS score, where 0 is Info, less than 4 is Low, less than 7 is Medium, less than 10 is High, and a CVSS score of 10 will be flagged as Critical[2].

Saint8[3] deals with assets, such as data, personnel, devices, systems and facilities that enable the organization to achieve business goals. Stakeholders are involved in risk identification and in providing data for computing both technical and business-related cybersecurity metrics, such as business unit, function, criticality and business cost impact. In addition, Saint uses CVSS score to create a risk profile to classify (prioritize) vulnerabilities. CVSS scores are grouped by severity levels: less than 4 corresponds to Potential risk factor, 4-7 scores map to Concern risk factor and 7-10 score to Critical.

Retina Security Scanner[5] assess risk and prioritizes remediation based on Real Risk strategy[27] in business context considering assets criticality and vulnerability exploitability (evaluated with the help of Core Impact®, Metasploit® and Exploit-db tools), CVSS, and other factors[20]. It is available as a standalone application or as part of Retina CS Enterprise Vulnerability Management. Retina CS version 5.7[6] introduces new asset risk analysis, allowing the decision maker to 'weight' the asset score based on either threat risks (i.e. vulnerabilities and attacks) or exposure risks (i.e. ports, shares, services, accounts). To normalize the risk according to a company's priorities a scale between 0 and 10 is introduced, with lowest score (0) corresponding to asset with lowest risk and with highest score (10) corresponding to asset with highest priority.

GFI LANGuard[7,8,23] scans the ICT infrastructure (hardware, network, operating systems, services, and applications), performs vulnerability analysis, risk assessment, and identifies and prioritizes remediation actions using

databases such as Open Vulnerability and Assessment Language (OVAL)[21] and SANS Top 20[22]. The tool also provides executive and technical reports for business and technical decision support.

nCircle IP360 and Tripware IP360[9,10] perform hosts data collection, vulnerability scoring and prioritization. Moreover, it also suggests remediation measures and prioritizes them. These tools make use of exploitability and vulnerability data from Tripwire's Vulnerability and Exposure Research Team (VERT). Business context is taken into account within risk assessment.

Security System Analyzer 2.0[11,24] (SSA) defines a patch management deployment strategy using CVSS scores to qualify the vulnerabilities. Also, SSA identifies vulnerabilities and discrepancies using the OVAL interpreter and performs compliance and security checks using the XCCDF - The eXtensible Configuration Checklist Description Format[25].

OpenVas[12,13] scanner shows the results of the vulnerabilities prioritized according to the impact on the systems (high, medium or low) and indicates the number of vulnerabilities found for each impact category. Besides OpenVAS is an official OVAL Adopter and OpenVAS-5 is registered as 'Systems Characteristics Producer'.

QualysGuard[14] manages cybersecurity vulnerability risks taking into account severity, business risk, CVSS scores, existence of exploits, malware and available patches. It provides easy and flexible ways for ICT infrastructure scanning and cyber risk reporting.

Nexpose[15] associates CVSS metrics to calculate the risk of a vulnerability on an asset. It has different risk strategies which are based on the formula in which factors such as likelihood of compromise, impact of commitment, and asset importance are calculated. Each formula produces a different range of numeric values. Many of the available risk strategies use the same factors in assessing risk, each strategy evaluating and aggregating the relevant factors in different ways. The common risk factors are grouped into three categories: vulnerability impact, initial exploit difficulty, and threat exposure. The factors that comprise vulnerability impact and initial exploit difficulty are the six-base metrics employed in the Common Vulnerability Scoring System (CVSS). Threat exposure data come from of three variables: Vulnerability age which is a measure of how long the security community has known about the vulnerability, Exploit exposure is the rank of the highest-ranked exploit for a vulnerability that measures how easily and consistently a known exploit can compromise a vulnerable asset and Malware exposure which is a measure of the prevalence of any malware kits, also known as exploit kits, associated with a vulnerability. The risk assessment strategies are: real risk, temporal plus risk, temporal risk, weighted risk and PCI ASV risk[16,17].

- Real Risk, the following formula is used to calculate the Real Risk scoring model[27]:

$$\text{Risk} = \frac{\text{CVSS Impact Metrics}}{\text{CVSS Likelihood Metrics}} \times \text{Exposure}\left(\begin{matrix}\text{Malware Kits}\\ \text{Exploit Rank}\end{matrix}, \text{time}\right) \tag{1}$$

- Temporal Plus, the following formula is used to calculate the Temporal Plus scoring model[26]:

$$\text{Risk} = \sqrt{t} \times \frac{(1+AV+C+I+A)}{(AC+Au)^2} \tag{2}$$

Where (t)is the time-based likelihood and represents the number of days since vulnerability publicly disclosed. The overall score increases with the number of days. The 'CVSS' values refer to the various base component vectors of the CVSS version 2 which is broken down into 6 metrics, including: Access Vector (AV); Access Complexity (AC); Authentication Required (Au); Confidentiality Impact (C); Integrity Impact (I) and Availability Impact (A)[17].

- Temporal, the following formula is used to calculate the Temporal scoring model[26]:

$$\text{Risk} = \sqrt{t} \times \frac{(AV+C+I+A)!}{(AC+Au)^2} \tag{3}$$

- Weighted[15,16], the Weighted risk model is based primarily on asset data and vulnerability types, and it emphasizes the following factors: 1) Vulnerability severity, ranging from 1 to 10; 2) Number of vulnerability instances; 3) Type of asset, such as a computer, router, or wireless access point (WAP); 4) Number and types of services on the asset; 5) The level of importance, or weight, that is assigned to a site when you configure it (e.g. low, high). The following formula is an algorithm defined in the Nexpose configuration files for the Weighted scoring mode, this file can be found as 'vulnsev-scvtype-devclass.xml'[28].

$$Risk = vulnSeverity \times 0{,}02 \quad (4)$$

- PCI ASV 2.0[26,30], this strategy applies a score based on the Payment Card Industry Data Security Standard (PCI DSS) Version 2.0 to every discovered vulnerability. PCI DSS specifies twelve requirements for compliance, among the requirements for risk assessment is defined 'Vulnerability Categorization' to assist in prioritizing the solution or mitigating identified issues. Approved Scanning Vendors (ASVs) must assign a severity level to each identified vulnerability (1 = lowest severity, 5 = highest severity) and must use two tools to categorize and rank vulnerabilities, and determine scan compliance: 1. The Common Vulnerability Scoring System (CVSS) version 2.0 and 2. The National Vulnerability Database (NVD). Any vulnerability with a CVSS base score of 4.0 or higher will result in a non-compliant scan

3. Risk assessment tools comparison

As described in the previous section each tool uses various techniques or strategies for risk-based prioritization. Most of these tools use CVSS score metrics to assess the risk that a vulnerability may pose to the business, either in the tool's own strategies or by adding new metrics that allow the user a better understanding of what is happening in the environment. In addition, to have more complete data for risk management, many of the tools have integration mechanisms with other commercial technology partners to further enhance the management of vulnerabilities that can affect an organization. Table 1 shows the tools comparison in terms of metrics, proposed strategies and if they support integration mechanisms with technology partners.

Table 1. Comparison of cyber security risk management tools.

Tool	Metric	Strategy	Integration mechanisms with
Nessus Home	CVSS2, CVSS3	Results based on the risk factor of the vulnerability (e.g., Low, Medium, High, Critical)	Kenna, ThreatConnect, Cisco ISE, ForeScout
Saint8	Business unit, Criticality, Business cost, CVSS	Prioritization and the application of resources to assets based on metrics of importance to the organization.	Cisco FireSIGHT Management Center
EyeRetina	Business impact, Core Impact, Metasploit, Exploit-db, CVSS	Real risk to critical assets and exploitability	Kenna, IBM QRadar SIEM, LogRhythm
GFILanguard	OVAL, CVE	Security issues are rated by their severity level and each computer is given a risk and vulnerability rating.	Core Security Technologies
nCircle® IP360	CVE, CVSS OVAL, SCAP	Prioritizes vulnerabilities, manages risk and improves security efficacy by combining business context with vulnerability intelligence.	Kenna, IBM QRadar, Bringa, LockPath, Trusted Integration
Security System Analyzer	CVE, CVSS, OVAL, SCAP	-	-
OpenVAs	OVAL	The results of the vulnerabilities prioritized according to the impact on the systems.	Kenna, Greenbone, SecPod
QualysGuard	CVSS, CVE, SCAP, Severity	Risk-based approach to prioritizing the remediation efforts and fixing those vulnerabilities that would impact the business.	Bringa, Modulo, Kenna, ForeScout LogRhythm

Nexpose	CVE, CVSS, SCAP	Real Risk, Temporal Plus, Temporal Weighted, PCI ASV 2.0	Kenna, ForeScout,LogRhythm Bringa,LockPath, Modulo,RSA Security Analytics, Risk I/O, TraceSecurity, Agiliance, R.sam

Although most of the tools use the CVSS metrics for prioritization and risk management, some of them incorporate other metrics considered important to an organization. For example, Saint8 incorporates 'Business unit', 'Criticality' and 'Business cost' to know the impact that a vulnerability may have on the business. Eye Retina uses 'Business impact', 'Core Impact Metasploit and Exploit db' as other metrics to assess risk, and QualysGuard uses severity levels based on the CVSS score. It is possible to emphasize that some of the tools pose their own risk assessment strategy to support decision making. Among them are nCircle® IP360 that combines business context with vulnerability intelligence, Saint 8 that associates not only the base metrics but also the environment metrics to measure the real risk impact on the organization, and Nexpose that incorporates different risk strategies adapted to the needs of the business. Another feature to note is the support for integration with other technology partners that different tools have. The technology partners provide a specialized service for risk assessment and decision support that also incorporates the results of the vulnerability scanning tool in a format compatible like XML - eXtensible Markup Language, making it more powerful for security and business value analyses. Most of the solutions provided by these technology partners are commercial or have a limited trial time, which represents a strong constraint for many companies.

4. Case Study

The case study presented in this paper was carried out at the 'Research Center of the Department of Computer Science of Universidad de las Fuerzas Armadas ESPE' in Ecuador. Nexpose was used to carry out a scan in the research center ICT infrastructure that allowed to analyze possible threats and to perform cybersecurity risk assessment. As described in the previous section, Nexpose offers the possibility to calculate risk using different strategies adjusted to the organization's environment, helping to prioritize the vulnerabilities that need to be addressed first. The study is focused on the comparison of different risk assessment strategies applied within the same case study. Table 2 shows the risk calculated by Nexpose, with a total of 49 vulnerabilities found, not considering criticality factor (CVSS environmental metrics).

Table 2. Nexpose Risk Scores

Strategy	Risk Score Original
Real Risk	17,920
Temporal Plus	48,048
Temporal	43,227
Weighted	10.0
PCI ASV 2.0 Risk	5.0

The criticality factor shows importance of an asset or its impact on business. In Nexpose this is identified by 'Criticality Tag'. Each criticality tag has an associated risk score modifier. The listed risk modifiers will be included in asset risk score calculations when 'Risk Score Adjustment' is enabled. These values can be adjusted according to the specific needs of the business. Fig. 1 shows Nexpose default values form adopted for the case study.

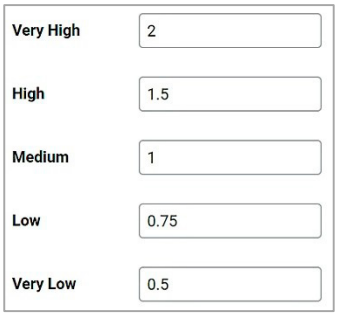


Fig.. 1. Risk Score Adjustment

In Nexpose, the risk score is applied to a site (asset or collection of assets that are targeted for a scan) or asset group. The calculation used to determine the risk for the entire site or group depends on the risk strategy. In addition, the criticality gets applied to each asset and the total risk score for the group is calculated based upon the individual asset risk scores. "To calculate the risk score for an individual asset, Nexpose uses the algorithm corresponding to the selected risk strategy. If 'Risk Score Adjustment' is set and the asset has a criticality tag applied, the application then multiplies the risk score determined by the risk strategy by the modifier specified for that criticality tag"[29]. The values presented in Table 3 were applied to a site with an asset (server), in each column can be observed the difference between the risk scores with respect to the applied criticality tag (see Fig.1) and the selected strategy. In case of having more than one asset could be compared the risk scores, the asset with the highest score will have higher priority.

Table 3. Risk Score Comparison

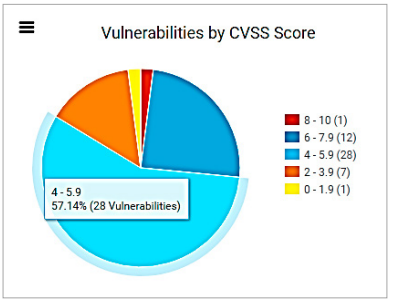
	Criticality				
Strategy	Very High	High	Normal	Low	Very Low
Real Risk	35,841	26,881	17,920	13,440	8,960
Temporal Plus	96,096	72,072	48,048	36,036	24,024
Temporal	86,454	64,840	43,227	32,420	21,613
Weighted	20.1	15.0	10.0	7.5	5.0
PCI ASV 2.0 Risk	10.0	7.5	5.0	3.8	2.5

Complementarily, Fig. 2 shows the report generated by Nexpose about the vulnerabilities found. This report allows the identification of vulnerabilities that may affect the organization most critically based on some most relevant criteria such as CVSS score, score according to risk strategy and severity.

Fig.. 2. Report vulnerabilities found

In addition, Nexpose offers different graphical reports to gain insights into what is happening in the organization environment as well as to understand how the vulnerabilities are affecting and jeopardizing the company's assets. One of the useful reports for an organization's cyber security team is the 'Vulnerabilities by CVSS score', which shows

the amount of vulnerabilities group by CVSS score ranges. Fig. 3 shows a Nexpose graphical report from the case study.



Fig,3. Vulnerabilities by CVSS Score

5. Proposal

This paper extends the proposal presented in [17] for the development of a decision support system for corporations cybersecurity management, following a context-aware systems layered model, i.e. addressing the perception, comprehension, projection and decision / action layers. As the result of comparing the cybersecurity risk analysis tools presented in previous sections and other publication from the same authors[17], Nexpose was selected as the most adequate tool to support the perception layer of the decision support system proposed. Currently only the perception and comprehension layers are developed and integrated with Nexpose, by the means of XML (eXtensible Markup Language) Nexpose reports data sharing and integration and a specific ontology designed to support the comprehension layer features of our proposed cybersecurity decision aiding system[17]. In Roldán at al.[17], an ontology design and a transformation process of Nexpose reports to an OWL ontology was implemented.

After the analysis performed in this paper on cybersecurity tools risk management and decision support features, we are able to extend the ontology proposed in our previous study to incorporate formal logics rules at the projection and decision/action layers. This allows for description logics inference ability and computation of metrics that have an impact on the organization.

The 'Security.owl' ontology of UNIK4710-owl project (available in GitHub)[18] will also be considered in our study because it promotes the interaction in a high level of abstraction between different security standards and annotations.

The ultimate goal of our proposal is to build a decision support system covering all context-aware layers, to provide support for chief information security officers to take appropriate decisions/actions in maintaining the security of the company.

6. Conclusions and future work

This paper presents a study for the development of a cybersecurity risk analysis and management system. The context-aware layered reference model was followed, addressing the perception, comprehension, projection and decision / action layers. A detailed analysis of the ICT infrastructure data collection features available in most relevant cybersecurity tools in this area was carried out. The cybersecurity risk strategies and metrics currently supported by each of those tools were also studied and compared. This study complements the work done in our 'A Decision Support System for Corporations Cybersecurity Management'[17] paper in relation to the projection and decision / action layers. A case study using the studied tools was carried out at 'Universidad de las Fuerzas Armadas ESPE' and presented with focus on cybersecurity metrics and risk strategies analysis.

As future work we propose to extend the ontology designed in 'A Decision Support System for Corporations Cybersecurity Management'[17] in order to specialize the risk analysis techniques of Nexpose, using the knowledge management features supported by OWL and adding new business related metrics such as cost, weight, impact and security pillars (confidentiality, integrity, availability), benefiting from the formal logics inference and reasoning and decision aiding features made possible by semantic technologies such as OWL, to meet cybersecurity specific corporations needs.

Acknowledgements

The present study is carried out as part of the Master's Degree in Computer Engineering - Mobile Computing at the Polytechnic Institute of Leiria, thanks to the scholarship granted by the agreement SENESCYT- Leiria Polytechnic Institute. Vitor Basto-Fernandes is supported by the Portuguese republic national funds through the Portuguese Foundation for Science and Technology (FCT - Fundação para a Ciência e a Tecnologia I.P) under the project UID/CEC/4524/2016.

References

1.Tenable, “Nessus 6.9 User Guide,” 28 April 2017. Available: https://docs.tenable.com/nessus/6_9/Content/Resources/PDF/Nessus_6_9.pdf.
2. Tenable Community, “Risk Factor,” 8 July 2010. Available: https://community.tenable.com/thread/2567.
3. Saint, “Asset Management,” 2017. Available: http://www.saintcorporation.com/products/asset-management/.
4. Saint, “SAINT 8 User Documentation,” 2014. Available: http://my.saintcorporation.com/resources/documentation/saint_documentation.pdf
5. BeyondTrust, “Retina Network Vulnerability Scanner,” 2017. Available: https://www.beyondtrust.com/products/retina-network-security-scanner/.
6. BeyondTrust, “Retina Enterprise Vulnerability Management Solutions,” 2017. Available: https://www.beyondtrust.com/wp-content/uploads/new-features-retina-cs-5-7-rnss-5-23.pdf?1448922701
7. GFISoftware, “GFILanguard,” 2017. Available: http://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard
8. BitWork Technologies, “Network Security Scanner and Patch Management,” 2012. Available: http://www.bitworktech.com/our-solutions/information-security/patch--vulnerability-management.
9. Tripwire, “Tripwire IP360: Enterprise-Class Vulnerability and Risk Management,” 2016. Datasheet.
10. Tripwire, “Prioritize Vulnerabilities, Manage Your Risk,” 2017. Available: https://www.tripwire.com/solutions/vulnerability-and-risk-management/.
11. Brothersoft, “Security System Analyzer 2.0 Beta002,” 14 November 2012. Available: http://www.brothersoft.com/security-system-analyzer-132933.html.
12. Welivesecurity., “Cómo utilizar OpenVAS para la evaluación de vulnerabilidades,” 18 November 2014. Available: https://www.welivesecurity.com/la-es/2014/11/18/como-utilizar-openvas-evaluacion-vulnerabilidades/.
13. OpenVas, “About OpenVAS Software,”. Available: http://www.openvas.org/software.html#feature_overview.
14. Qualys, Inc, “Vulnerability Management,” 2017. Available: https://www.qualys.com/suite/vulnerability-management/features/#prioritize.
15. Rapid7Community, “Nexpose User's Guide (English),” 26 April 2017. Available: https://community.rapid7.com/docs/DOC-1387.
16. Rapid7Community, “Working with risk strategies to analyze threats,” Available: https://help.rapid7.com/nexpose/en-us/Files/Working_with_risk_strategies_to_analyze_threats.html.
17. G. Roldán-Molina, M. Almache-Cueva, C. Silva-Rabadao, V. Basto-Fernandes e I. Yevseyeva, “A Decision Support System for Corporations Cybersecurity Management,” 12th Iberian Conference on Information Systems and Technologies, Lisboa-Portugal, 2017. Published
18. JosefNoll, “Ontologies for course UNIK4710,” 11 April 2013. Available: https://github.com/unikdrift/UNIK4710-owl.
19. FIRST.org, Inc., “Common Vulnerability Scoring System, V3 Development Update,” 2017. Available: https://www.first.org/cvss
20. BeyondTrust, “Retina CS EnterpriseVulnerability Management,” 2017.Available:https://www.beyondtrust.com/wp-content/uploads/ds-retina-cs.pdf?1486141809
21. The Mitre Corporation, “OVAL Open Vulnerability and Assessment Language,”9 February 2016. Available: https://oval.mitre.org/.
22. SANS™ Institute, “SANS Critical Security Controls Poster,” 2014. Available: https://www.sans.org/media/critical-security-controls/Poster_Fall_2014_CSCs_WEB.PDF.
23. Insight Technology Solutions Aps, “GFI LANguard,” 2017. Available: http://dk.insight.com/shop/gfi/languard
24. Google Code, "SA - Security System Analyzer 2.0," 2016. Available: https://code.google.com/archive/p/ssa.
25. Nist, “XCCDF - The Extensible Configuration Checklist Description Format,” 16 December 2016. Available: https://scap.nist.gov/specifications/xccdf/.
26. Rapid7, “PCI, CVSS, & risk scoring frequently asked questions,” 14 December 2016. Available: https://help.rapid7.com/nexpose/en-us/Files/Risk_scoring_FAQ.html
27. Rapid7, “Leveraging Security Risk Intelligence,” July 2014. Available: https://information.rapid7.com/rs/495-KNT-277/images/rapid7-whitepaper-leveraging-security-risk-intelligence.pdf
28. Rapid7Community, “Creating custom NeXpose risk scoring strategies,” 10 April 2011. Available: https://community.rapid7.com/docs/DOC-1136
29. Rapid7Community, “Adjusting risk with criticality,” 2017. Available: https://help.rapid7.com/insightvm/en-us/index.html#Files/Adjusting_risk_with_criticality.html#criticality_strategy_interaction
30. PCI Security Standards Council LLC, “Payment Card Industry (PCI) Data Security Standard Approved Scanning Vendors,” 2013. Available: https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v2.pdf